Haaga-Helia
ammattikorkeakoulu Oy

Julkisten WLAN-Verkkojen tietoturva yksityishenkilön näkökulmasta

Jere Vatka

Opinnäytetyö
Tietojenkäsittely
2016

Tiivistelmä

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t)
Jere Vatka

Koulutusohjelma
Tietojenkäsittely

Opinnäytetyön otsikko
Julkisten WLAN-Verkkojen tietoturva yksityishenkilön näkökulmasta

Sivu- ja liitesivumäärä
28 + 1

Tämän opinnäytetyön tarkoituksena on tuoda esille yksityishenkilölle esiintyvät riskit julkisissa langattomissa lähiverkoissa. Tämän lisäksi opinnäytetyössä käydään läpi menetelmiä, joilla yksityishenkilö voi suojata omaa yhteyttään käyttäessään julkisia langattomia lähiverkkoja.

Opinnäytetyössä on rajattu pois yritykset ja yhteisöt. Työ on myös laadittu lukijalle kevyeksi ja sanastoa karsittu pois siitä syystä, että asiasta vähemmän ymmärtävät lukijat pystyvät hyödyntämään työtä oman tietoturvansa parantamiseksi.

Tässä työssä käsitellään ensiksi julkisten langattomien verkkojen mukanaan tuomia tietoturvariskejä. Tämän jälkeen työssä pyritään löytämään ennaltaehkäiseviä ratkaisuja esiin tulleisiin tietoturvaongelmiin. Lopuksi luodaan yhteenveto ja tuodaan esille johtopäätökset.

Syy langattomien lähiverkkojen tietoturvaongelmiin on se, että se suunniteltiin toiminnallisuus edellä ja tietoturvaan ei luomisvaiheessa kiinnitetty huomiota. Suurimpana ongelmana voidaan pitää sitä, että langattomissa verkoissa data kulkee radiosignaaleina ilmateitse, jolloin niitä voidaan siepata kenen tahansa toimesta.

Työn johtopäätöksenä voidaan sanoa, että julkisissa WLAN-verkoissa suojaus on aina käyttäjän vastuulla. Tämä johtuu siitä, että verkon tarjoajat haluavat yhteyden muodostamisen olevan mahdollisimman helppoa ja vaivatonta. Mikäli käyttäjä ei ymmärrä suojata yhteyttään, on hänellä suuri todennäköisyys joutua rikoksen uhriksi. Nämä rikokset ovat erittäin huolestuttavia, koska käyttäjän luotettava yksilöllinen identifiointi julkisessa verkossa on lähestulkoon mahdotonta. Se tarkoittaa, että rikoksista ei ikinä saada tekijää selville.

Asiasanat
Tietoturva, WLAN, Langaton lähiverkko

Sisällys

1 Johdanto 1
1.1 Tavoitteet 2
1.2 Rajaukset 2
1.3 Keskeisiä käsitteitä 3
2 Langattomat lähiverkot 5
2.1 Historia 5
2.2 Toiminnallisuus 6
2.3 Yhteydet 7
2.4 WLAN-Verkkojen topologia 9
3 Tietoturvariskit 10
3.1 Luvaton tunkeutuminen verkkoon (Breaking into a network) 11
3.2 Mies välissä -hyökkäys (Man in the Middle Attack) 12
3.3 Palvelunestohyökkäys (Denial of Service) 13
3.4 Identiteettivarkaus (MAC-Spoofing) 14
3.5 Verkkourkinta (Phishing) 15
4 Julkisten WLAN-verkkojen tietoturvauhkien minimointi 16
4.1 Käyttäjän asennoituminen tietoturvauhkiin 17
4.2 Virtual Private Network (VPN) 17
4.3 Kaksivaiheinen tunnistautuminen 18
4.4 Salattu yhteys 19
4.5 Tukiaseman asetukset 20
4.6 Lokitiedostot 20
5 Johtopäätökset 22
Lähteet 24
Liitteet 29
Liite 1. Tietoturvaohjeet yhdistäessä julkiseen langattomaan lähiverkkoon 29

1 Johdanto

Tämä opinnäytetyö käsittelee julkisten langattomien lähiverkkojen taustaa, tietoturvariskejä ja niiltä suojautumista. Langattomien verkkojen määrä yksityiskäytössä ja julkisessa käytössä on lisääntynyt merkittävästi viime vuosina. Wi-Fi teollisuuden äidin, Wi-Fi Alliance:n mukaan vuonna 2013 oli myyty yli 2 miljardia langatonta lähiverkkolaitetta ja langattomia verkkoja oli 25% koko maailman talouksissa. Strategy Analytics tutkimuksen mukaan vuonna 2016 noin 800 miljoonassa taloudessa olisi WLAN. (F-Secure 2014, 6-8.)

Julkisella puolella Wi-Fi hotspotit ovat yleistyneet mahdollistaen asiakkailleen nopean ja helpon tavan yhdistää omat laitteensa langattomaan verkkoon, ja tarjoten mahdollisuuden käyttäjälle päästä sosiaaliseen mediaan. Kova kasvu ei ole ainoastaan asiakkaiden vaatimusten ansiota, vaan on todettu, että se parantaa myös liiketoimintaa. (F-Secure 2014, 6-8.) Esimerkiksi kirjakaupat, kahvilat ja ravintolat hyödyntävät yleensä yksinkertaista ja ilmaista hotspottia, jotta he saisivat asiakkaat jäämään liikkeeseen pidemmäksi aikaa, mikä puolestaan johtaa suurempaan myyntiin. Hotellille on myös huomattavasti edullisempaa ylläpitää langatonta verkkoa kuin langallista verkkoa. (Fisher 2005, 5.)

Nykyään ilmaisia hotspotteja pidetään jo itsestäänselvyytenä kahviloissa, hotelleissa, ostoskeskuksissa, kirjastoissa, lentokentillä ja baareissa, eivätkä niihin kirjautuvat asiakkaat kyseenalaista niiden turvallisuutta millään tavalla. Mutta niin kuin Internetkin, myös WLAN kärsii synnynnäisestä heikkoudesta: sitä ei alun perin suunniteltu turvallisuutta ajatellen. Päätavoitteena oli vain pystyä luomaan yhteys. (F-Secure 2014, 6-8.)

Langattomien verkkoyhteyksien suurimpana ongelmana voidaan pitää sitä, että tietojen siirrossa käytettävä radiotaajuuksilla toimiva yhteys on perinteistä langallista yhteyttä riskialttiimpi. Radioaaltoja voi kuka tahansa siepata, jos yhteys jätetään suojaamatta. (Symantec 2016.) Monien langattomien verkkojen tietoturva on kuitenkin heikosti toteutettu. Syy siihen on, että useissa tapauksissa verkkojen suojaukseen ei viitsitä kiinnittää huomiota, tai välttämättä edes osata parantaa niiden turvallisuutta.

Julkisia lähiverkkoja käytettäessä on useita tapoja suojata käyttäjää ulkopuolisten hyökkäyksiltä ja varmistaa turvallinen yhteys. Tässä opinnäytetyössä selvitetään erilaisia tietoturvauhkia julkisia langattomia lähiverkkoja käytettäessä sekä mahdollisuuksia, joilla parantaa yksityishenkilön tietoturvaa yhdistäessä ja käytettäessä näitä verkkoja.

1.1 Tavoitteet

Opinnäytetyön tavoitteena on kartoittaa, kuinka julkisen verkon käyttö voi vahingoittaa yksityishenkilöä ja kuinka yksityishenkilön tietoturvaa voidaan parantaa julkisissa verkoissa. Työn tarkoituksena on myös muotoutua tietoturvaa parantavaksi kokonaisuudeksi, joka hyödyttää myös vähemmän tietotekniikasta ja langattomista verkoista tietäviä lukijoita. Työssä menettelytapana on tiedonkeruu lähteistä. Tämä työ on kirjallisuuskatsaus ja sen tarkoituksen puolesta ei ole tehty empiiristä tutkimusta.

1.2 Rajaukset

Opinnäytetyössä käsitellään aihetta yksityishenkilön henkilökohtaisen tietoturvan näkökulmasta, jolloin erilaiset yritykset ja yhteisöt ovat rajattu pois. Yritysten ja yhteisöjen näkökulmat on rajattu pois myös siitä syystä, ettei opinnäytetyö kasvaisi liian laajaksi. Langattomissa verkoissa käytettävien laitteiden ja ohjelmistojen teknisiä yksityiskohtia ja käsitteitä käsitellään siten, että myös aiheesta hieman vähemmän tietävät lukijat pystyvät tämän opinnäytetyön perusteella käyttämään julkisia langattomia lähiverkkoja turvallisemmin. Tämän takia työ on haluttu pitää mahdollisimman kevyenä ja helposti luettavana, mistä johtuen esimerkiksi langattomien verkkojen radiotekniset yksityiskohdat ovat myös rajattu pois. Lisäksi työstä on rajattu pois erillisten palomuurien sekä virustorjunnan vaikutukset yksityishenkilön tietoturvaan, sillä ne eivät ole kiinteästi yhteydessä langattoman verkon tietoturvaan.

1.3 Keskeisiä käsitteitä

Hotspot on fyysinen paikka, missä käyttäjä voi yhdistää oman lähiverkkolaitteensa internettiin Wi-Fi teknologiaa hyödyntäen. Se tapahtuu WLAN-verkon kautta, joka on yhdistettynä internet palveluntarjoajaan.

Langaton lähiverkko eli WLAN (englanniksi “Wireless Local Area Network”) on suosittu, edullinen ja yksinkertainen tapa luoda yhteys internetiin. Yhteys voidaan luoda kahden langattoman verkon verkkolaitteen välille ilman kaapelointia. Langattomassa verkossa tieto siirtyy radiosignaalin välityksellä laitteesta toiseen, joka mahdollistaa käyttäjälle vapaamman ja joustavamman verkon käytön. Fyysisesti WLAN-verkko rakentuu verkon tukiasemasta, joka liitetään kiinteään langalliseen tietoverkkoon. Sen avulla tukiasema jakaa internet-verkkoa langattomasti kyseisen verkon päätelaitteille. WLAN terminä viittaa yleensä IEEE 802.11 -standardiin. (Viestintävirasto 2014.)

MAC-osoite eli Media Access Control on yksilöllinen koodi, joka on määritetty tietylle verkkolaitteiden ryhmälle valmistajan johdosta.

Tukiasema on laite, joka yhdistää langattomassa tietoliikenteessä päätelaitteen radioteitse kiinteään, langalliseen runkoverkkoon. Tämä puolestaan mahdollistaa pääsyn verkon ulkopuolelle, esimerkiksi internetiin. Tukiasema toimii lähettimenä ja vastaanottimena tietyllä alueella. Langattomassa verkossa voi olla useampia tukiasemia, jolloin langattoman verkon kuuluvuusalue suurenee. Useamman tukiaseman verkossa käyttäjä voi halutessaan liikkua eri tukiasemien kuuluvuusalueella ilman, että verkkoyhteys katkeaa. (Viestintävirasto 2014.)

Tietoturva pyrkii suojaamaan yksityishenkilölle tärkeät tiedot ulkopuolisilta. Tietoturvalla tarkoitetaan menetelmiä, joilla turvataan yksityishenkilön tietojen koskemattomuus. Tietoturvallisuus rakentuu asetetuista tavoitteista, joiden avulla kokonaisuutta on helpompi seurata. Näitä tavoitteita ovat *luottamuksellisuus*, *eheys*, *kiistämättömyys*, *pääsynvalvonta*, *saatavuus* ja *tarkastettavuus*. (Internetopas 2016.)

Luottamuksellisuus tarkoittaa sitä, että tiedot, järjestelmät ja palvelut ovat vain niihin oikeutettujen henkilöiden käytössä. Turvaluokitus määrittelee tietojen osalta sen, kenellä on oikeus käyttää tietoa, muuttaa sitä tai tuhota se kokonaan. *Eheys* tarkoittaa tiedon muuttumattomuutta sen luomisen, käsittelyn ja siirron aikana. *Kiistämättömyydellä* varmistetaan, ettei kukaan voi kiistää osuuttaan tietojen siirtoon tai käsittelyyn jälkikäteen. Osallisten tunnistautumista valvotaan tiedon käsittelyn ajan. (Internetopas 2016.)

Pääsynvalvonnalla rajoitetaan ja valvotaan käyttäjien pääsyä tietoon. Tietojärjestelmä ja sen tiedot eivät ole sellaisten henkilöiden käytettävissä, joilla ei ole käyttöoikeutta kyseisiin tietoihin. *Saatavuus* puolestaan tarkoittaa tiedon yksinkertaista, virtaviivaista ja helppoa käyttöä niille henkilöille, joilla on siihen käyttöoikeus. *Tarkastettavuus* tarkoittaa, että muodostuneen tiedon alkuperä pitää voida tutkia ja selvittää esiintyykö tiedossa virheitä tai epäsäännöllisyyttä sekä tarkistaa tiedon oikeellisuus. (Internetopas 2016.)

Wi-Fi on vain Wi-Fi Alliancen luoma tavaramerkki päätelaitteille, jotka hyödyntävät IEEE 802.11 -standardia. Yleinen väärinkäsitys on, että Wi-Fi olisi lyhenne sanoista “Wireless Fidelity”, eli langaton täsmällisyys, mutta asia ei ole näin. (Webopedia 2016a.)

2 Langattomat lähiverkot

Langaton lähiverkko toimii samalla tavalla kuin langallinen lähiverkko, ainoa ero on tiedonsiirrossa käytettävä menetelmä. Kun langallisessa lähiverkossa data siirtyy kaapelia pitkin, langattomassa lähiverkossa data siirtyy radiosignaaleja käyttäen radiotaajuuksilla. Tästä johtuen langaton lähiverkko on huomattavasti riskialttiimpi kuin kiinteä verkko, jossa voidaan vaikuttaa siihen, kenellä on pääsy verkkoon. Ihmiset kuitenkin halusivat ja tarvitsivat nopeamman ja yksinkertaisemman tavan yhdistää itsensä lähiverkkoon, sillä fyysiset kaapelit ovat suhteellisen hidas ja hankala sekä se vaatii vapaan paikan reitittimestä. Tuloksena syntyi 1990-luvulla langaton teknologia nimeltään Wi-Fi, joka oli ensimmäinen tehokas ratkaisu langattoman verkon käyttöönotolle. (Sans Institute 2015b, 1-3.)

2.1 Historia

Ensimmäinen langaton lähiverkko syntyi, kun koulut ja yritykset uskoivat pystyvänsä laajentamaan heidän tietojenkäsittelyalueitaan laajentamalla langallisia lähiverkkoja (LAN) hyödyntäen langattomia lähiverkkoja (WLAN). Tämä ensimmäinen WLAN syntyi 1971 Hawaiin yliopistossa, kun tietoverkot kohtasivat radioyhteydet projektissa ALOHAnet Norman Abramsonin johdolla. (John Hopkins School of Public Health 2007.)

Vuonna 1990 IEEE (Institute of Electrical and Electronics Engineers) aloitti ensimmäisen langattoman lähiverkon standardin kehittämisen ja vuonna 1997 julkaistiin ensimmäinen varsinainen standardi IEEE 802.11. Tällä standardilla oli yhteensopivuusongelmia laitteiden kanssa sekä taajuuskaistaan liittyviä lupaongelmia. Pohja oli kuitenkin niin hyvä, että sen päälle alettiin kehittää uusia standardeja. Jo 1990-luvun lopulla lähes kaikki WLAN ratkaisut ja alkuperäiset protokollat olivat korvattu IEEE 802.11 standardin moninaisilla versioilla (versioista “a”: sta “n”: ään). (Technopedia 2016.)

Vuonna 1999 useat verkkolaitteiden kanssa tekemisissä olevat yritykset perustivat voittoa tavoittelemattoman yhtiön keskenään nimeltä Wi-Fi Alliance. Nykypäivänä mukana on jo yli 600 yritystä mukaan lukien Apple, Cisco, Samsung, Intel, Microsoft ja Sony. Sen tavoitteena on maailmanlaajuisen yhdenmukaisen WLAN-standardin käyttöönotto. Wi-Fi Alliancen tehtävänä on ajaa langatonta teknologiaa ja sovelluksia eteenpäin, sekä myöntää langattomille verkkolaitteille sertifikaatteja laitteiden niiden tukemien WLAN-standardien mukaisesti. Heidän brändinsä “Wi-Fi” on yleisesti käytetty termi IEEE 802.11x-standardeille, ja usein sekoitetaan WLAN-termiin puhekielessä. (Wi-Fi Alliance 2016; Technopedia 2016.)

1990-luvun alulla WLAN-verkot olivat todella kalliita ja epäkäytännöllisiä ja niitä käytettiin vain kuin langallinen verkko oli lähestulkoon mahdoton toteuttaa. Kun suuret yhtiöt alkoivat kehittää langattomia verkkoja, niiden hinta laski radikaalisti ja tästä syystä langattomat verkot alkoivat yleistymään myös yksityishenkilöiden käytössä. (Technopedia 2016.)

2.2 Toiminnallisuus

WLAN-verkko ajaa saman asian kuin LAN-verkko; se yhdistää ryhmän päätelaitteita toisiinsa. Se toimii radiotaajuuksilla hyödyntäen radiosignaalia. Nämä päätelaitteet ovat yhteydessä WLAN-verkon ytimeen eli tukiasemaan. Tukiasema lähettää verkkoa langatonta signaalia tietylle alueelle, jonka sisällä päätelaitteet löytävät sen ja näin yhdistyvät verkkoon. Päätelaitteita ovat esimerkiksi matkapuhelimet, printterit, tietokoneet ja tabletit. Päätelaitteen tehtävä on muuntaa käyttäjän tieto tietoliikenneyhteyden läpi lähetettäväksi signaaleiksi ja toimia dataa lähettävänä asemana, joka välittää signaalia linkkiprotokollan mukaan. Tukiasema on puolestaan laite, joka yhdistää langattomassa tietoliikenteessä päätelaitteen radioteitse kiinteään, langalliseen runkoverkkoon. Langatonta verkkoa voidaan laajentaa lisäämällä tukiasemia alkuperäisen tukiaseman kantoetäisyydelle. Liikkuessa verkossa, jossa on useampia tukiasemia, päätelaite vaihtaa itsestään tukiasemaa tarvittaessa yhteyden turvaamiseksi. Seuraavalla sivulla on kuva langattoman verkon tukiasemasta. (Webopedia 2007b; Viestintävirasto 2014.)

Kuvio 1: Langattoman verkon tukiasema RT-AC66U (Asus 2016.)

2.3 Yhteydet

Langatonta lähiverkkolaitetta hankkiessa törmää usein suorituskykyä ja nopeutta mittaaviin numeroihin, jotka taas puolestaan pohjautuvat laitteen tukemiin langattoman verkon standardeihin ja muihin lisäyksiin. Nämä numerot ovat yleensä todella optimistisia, eikä laitteilla todellisuudessa päästä kuin maksimissaan puoleen mainostetusta nopeudesta. Tietenkin signaali on vahvempi mitä lähempänä tukiasemaa ollaan. Seuraavalla sivussa olevassa taulukossa ovat IEEE 802.11 -protokollien nopeudet sekä kantoetäisyydet. (Webopedia 2016b.)

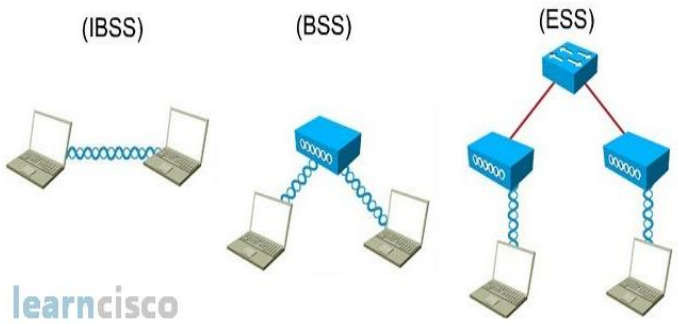
Taulukko 1. IEEE 802.11 -standardien protokollat, niiden julkaisuvuodet, nopeudet ja kantavuudet. (Wikipedia 2016.)

802.11 Protocol	Release date	Data rate (max)	Range (In-door)	Range (Out-door)
Legacy	1997	2 Mbit/s	20m	100m
802.11a	1999	54 Mbit/s	35m	120m
802.11b	1999	11 Mbit/s	35m	140m
802.11g	2003	54 Mbit/s	38m	140m
802.11n	2009	150 Mbit/s	70m	250m
802.11ac	2013	780 Mbit/s	35m	-
802.11ad	2012	6.75 Gbit/s	60m	100m
802.11ay	Est. 2017	100 Gbit/s	60m	1000m

Julkisessa verkossa ollessa pitää aina ottaa huomioon myös käyttäjien määrä, kun suunnitellaan nopeuksia. Langaton lähiverkko jaetaan yhdestä tukiasemasta kaikkien siinä asioivien päätelaitteiden kesken, joka luonnollisesti tarkoittaa sitä, että mitä enemmän laitteita on kyseisessä verkossa, sen vähemmän jokainen laite pystyy vastaanottamaan ja lähettämään dataa. (Webopedia 2016b.)

2.4 WLAN-Verkkojen topologia

Langattomat lähiverkot ovat IEEE 802.11 -standardin myötä tulleet joustavaksi toteutuksen kannalta. Verkkoja voidaan toteuttaa kolmella tavalla. Yksinkertaisin mahdollisista toteutustavoista on IBSS (Independent Basic Service Set) eli tilapäisverkko, jossa kahden tai useamman tietokoneen verkkolaitteet keskustelevat suoraan toistensa kanssa erillistä tukiasemaa. IBSS verkkoa usein kutsutaan adhoc verkoksi, koska se on pohjimmiltaan yksinkertainen vertaisverkko. Toinen tapa on tukiasemaan perustuva BSS (Basic Service Set), jossa langattomat WLAN-laitteet yhdistetään toisiinsa erillistä tukiasemaa käyttäen. Kaikki kommunikointi laitteiden välillä kulkee tämän tukiaseman lävitse. BSS-verkon tukiasema voi myös olla liitettynä suoraan langalliseen runkoverkkoon, jolloin voidaan mahdollistaa yhteys Internetiin. Tällaista BSS-verkkoa kutsutaan infrastruktuuriseksi BSS-verkoksi. Tämä infrastruktuuriin eli kiinteään tukiasemaan perustuva menetelmä on koti- ja yritysverkoissa yleisin käytössä oleva menetelmä. Tukiasemaan perustuva BSS-verkkoa on myös mahdollista laajentaa yhdistämällä useamman BSS-verkon. Tällöin kyseistä verkkoa kutsutaan nimellä ESS (Extended Service Set). Verkon laajennus voidaan tehdä joko langattomasti tai kytkemällä laajennus samaan runkoverkkoon kuin muut tukiasemat. Alla olevassa kuviossa on havainnollistettu WLAN-verkkojen topologiat.



Kuvio 2. WLAN-verkkojen topologiat. (Cisco 2016.)

Kuviossa 2. näkyvät siniset laatikot, joiden kyljessä on yhteyden kuva, ovat tukiasemia.

3 Tietoturvariskit

Yhä useammat ihmiset saavat töistään verkkolaitteen, tai käyttävät omaa verkkolaitettaan työasioiden hoitoon ja arkisiin asioihin, kuten sähköpostiin ja sosiaaliseen mediaan. Tämä elektroniikka seuraa meitä nykypäivänä kaikkialle ja ajaa ihmiset tarkistamaan esimerkiksi tärkeän työsähköpostin tilanteesta riippuen vaikkapa kahvilassa. Jos mobiilidatayhteyttä ei ole tai siitä ei haluta maksaa, yhdistetään luonnollisesti ilmaiseen langattomaan lähiverkkoon, mikäli se on saatavilla. Kun yhteys on luotu, on itse asiakas, mutta myös koko yritys vaarassa, mikäli käytössä on yrityksen tarjoama verkkolaite, joka sisältää yritykselle arvokasta tietoa. (Fisher 2015, 5-8.)

Perinteisessä langallisessa lähiverkossa tieto kulkee kaapeleita pitkin ja tällöin verkon fyysistä tietoturvaa on helppo valvoa. Langattomassa verkossa samaa fyysistä tietoturvaa on mahdotonta valvoa, koska tieto kulkee radiosignaaleina ilmateitse. Nämä signaalit kulkeutuvat usein myös normaaleiden ulkoseinien ja huoneistojen väliseinien läpi huomattavasti pidemmälle alueelle kuin niiden alkuperäinen tarkoitettu kantoalue. Tästä johtuen suojaamaton WLAN-verkko saattaa ulottua kymmeniäkin metrejä liiketilojen ulkopuolelle ja rikollista toimintaa voidaan toteuttaa ulkona liikkeestä, mahdollisia valvontakameroita väistäen. (Hamid 2003.)

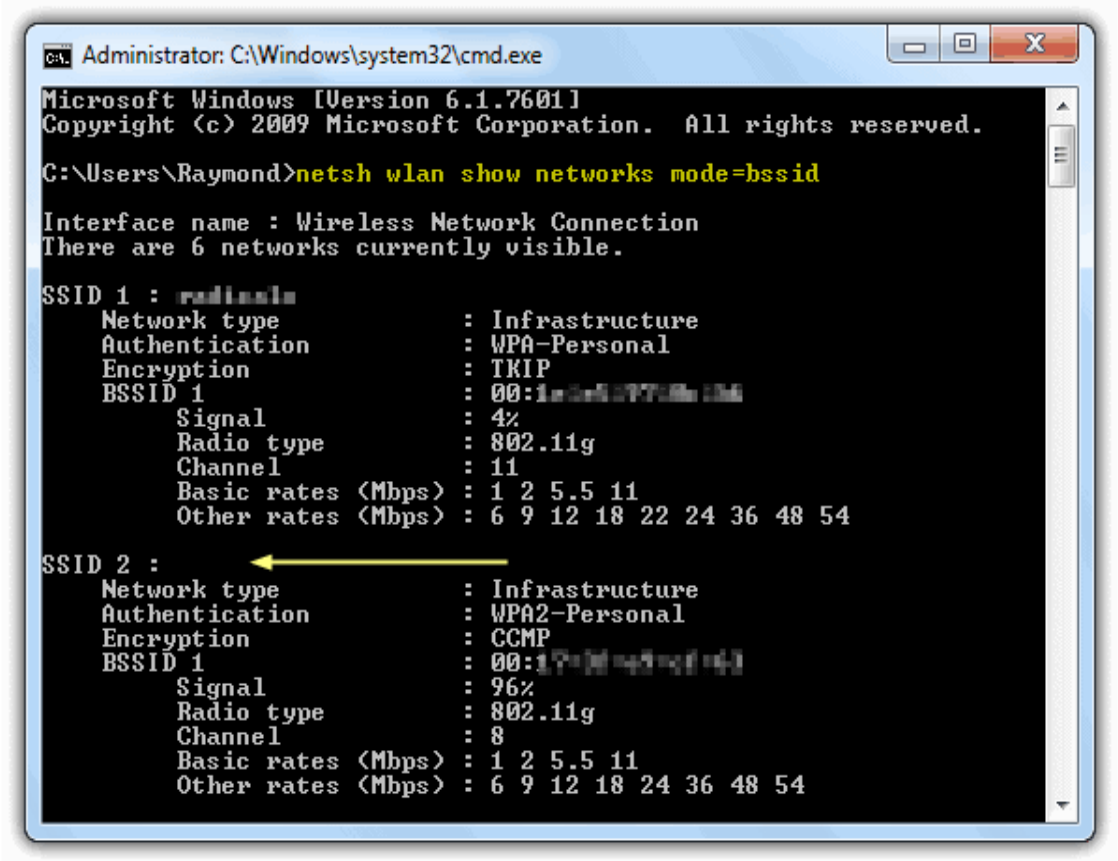
Julkista WLAN-verkkoa käytettäessä tulisi aina varmistaa, että tietokoneen palomuuri ja virustorjuntaohjelmisto ovat ajan tasalla. Esimerkiksi sähköpostia tulisi käyttää vain SSL-salatulla yhteydellä. Tämän lisäksi julkisesta verkosta ei kannata yhdistää arkaluontoisille Internet-sivuille, koska langattoman verkon tarjoaja yleensä ylläpitää rekisteriä ja seuraa liikennettä lokitiedostojen avulla.

Tässä osiossa tarkoituksena on käydä läpi suurimmat tietoturvauhkat, joita kohtaa julkisissa langattomissa verkoissa.

3.1 Luvaton tunkeutuminen verkkoon (Breaking into a network)

Luvaton tunkeutuminen langattomaan verkkoon alkaa siitä, että tunkeutuja etsii kyseiseltä alueelta WLAN-verkot ja selvittää niiden nimet. Tälle verkkojen etsinnälle käytetään kansainvälistä termiä “**War Driving**”. Termi on saanut nimensä siitä, että siinä henkilö ajaa autolla ympäriinsä samalla etsien avoimia langattomia verkkoja. Langattomien verkkojen etsintä on helppo ja suosittu hyökkäystapa, johtuen sen vähäisistä laitteisto- ja ohjelmistovaatimuksista. Kaikki mitä hyökkäykseen tarvitaan ovat kannettava tietokone, langaton verkkokortti, hyökkäykseen tarkoitettu ohjelma ja toimiva auto. Lisäksi voidaan käyttää GPS-laitteita paikan sijainnin merkitsemistä varten sekä lisäantennia langattoman verkkokortin kantosäteen kasvattamiseksi. (Wardrive 2016.)

Kun Wardrive on suoritettu, hyökkääjällä on kymmeniä, jopa satoja erillisiä langattoman verkon tukiasemia, joista hän tietää kenelle mikäkin kuuluu ja missä ne tarkalleen sijaitsevat. Kun verkko johon tunkeudutaan on valittu, alkaa itse tunkeutuminen. Piilotettuun verkkoon pääsee käsiksi esimerkiksi lähettämällä verkon kantoetäisyydellä jollekin laitteelle signaalin, jonka tukiasema lähettäisi, mikäli se olisi sammumassa. Kun kyseinen laite yhdistetään tämän jälkeen verkkoon, se löytää automaattisesti verkon SSID (Service Set Identifier), joka mahdollistaa verkkoon tunkeutumisen. Mikäli tunkeutuja pääsee käsiksi tukiaseman pääsynhallintaan, voi hän muuttaa mielivaltaisesti tukiaseman asetuksia tai halutessaan jopa tehdä tukiasemasta täysin käyttökelvottoman, jolloin kukaan asiakkaista ei pysty hyödyntämään verkkoa. Seuraavalla sivulla olevassa kuvassa on löydetty piilotettu verkko. (Hoffman 2016.)



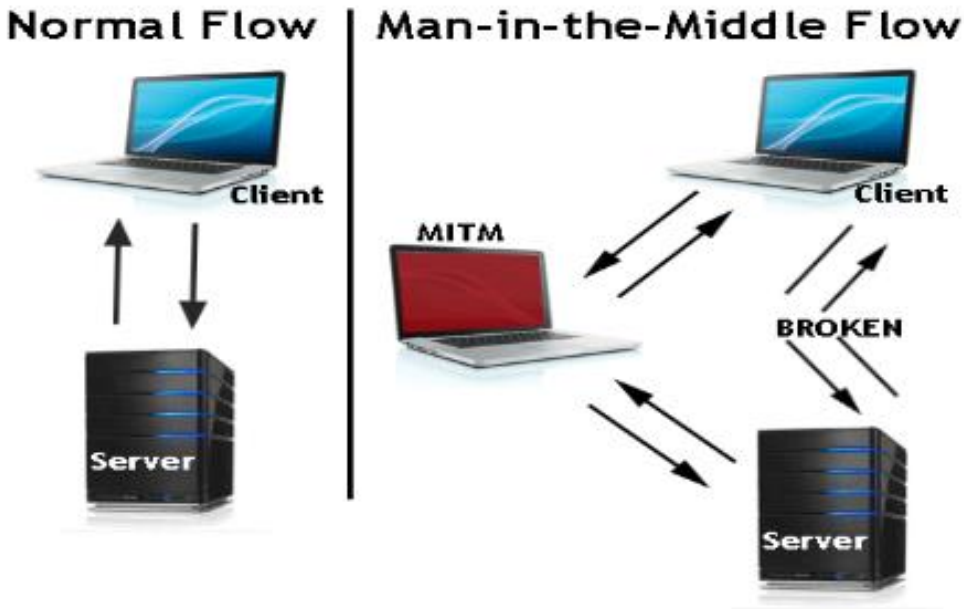
Kuvio 3. Piilotettu SSID-tunnus langattomassa lähiverkossa. (Raymond 2017.)

Kuviossa 3. näkyy kuinka War Drive :a suorittamalla voidaan löytää erilaisia verkkoja, joita on esimerkiksi pyritty suojaamaan SSID-tunnuksen piilottamisella.

3.2 Mies välissä -hyökkäys (Man in the Middle Attack)

Mies välissä -hyökkäyksellä tarkoitetaan sitä, että hyökkääjä asettautuu salaa kahden osallisen väliin, jakaa ja mahdollisesti jopa muuttaa kommunikointia näiden kahden osallisen kesken. Julkisessa verkossa se yleensä tarkoittaa sitä, että hyökkääjä sijoittautuu verkon käyttäjän, eli uhrin, ja verkon varsinaisen tukiaseman väliin. Jotta Mies välissä -hyökkäys voidaan toteuttaa, täytyy hyökkääjän valetukiaseman olla lähempänä uhria kuin varsinaisen tukiaseman. Hyökkäyksen aikana itse hyökkääjä esittäytyy uhrille olevansa verkon varsinainen tukiasema, johon uhrin tulee olla yhteydessä päästäkseen hyödyntämään palveluita. Samaan aikaan

hyökkääjä esittää verkon varsinaiselle tukiasemalle olevansa täysin tavallinen verkon käyttäjä. Kaikki data, muun muassa uhrin salausavaimet ja muut arkaluontoiset tiedot reitittyvät hyökkääjän kautta itse tukiasemaan. Alla olevassa kuvassa on havainnollistettu Mies välissä -hyökkäys. (F-Secure 2014; DuPaul 2016.)



Kuvio 4. Mies välissä -hyökkäys. (Veracode 2016.)

Kuviossa 4. on vasemmalla puolella normaali tila, missä verkon käyttäjä on suoraan yhteydessä palvelimeen. Oikealla puolella tapahtuu Mies välissä -hyökkäys. Yhteys käyttäjän ja palvelimen välillä on katkennut, ja yhteys muodostuu ylimääräisen tahon kautta, joka siis reitittää kaiken datan käyttäjän ja palvelimen välillä.

3.3 Palvelunestohyökkäys (Denial of Service)

Palvelunestohyökkäyksen tavoitteena on haitata verkon tarkoitettua toimintaa siten, että hyökkääjä lähettää valtavan määrän tietoliikennepaketteja langattomaan verkkoon hyvin lyhyellä aikavälillä. Koska verkko ei pysty käsittelemään paketteja yhtä nopeasti, kun niitä lähetetään, seurauksena on verkon toiminnan hidastuminen tai jopa täysi pysähtyminen. Tätä hyökkäystapaa kutsutaan tulvahyök-

käykseksi (eng. **flooding**), ja se on yksi tapa suorittaa palvelunestohyökkäys. Toinen hyökkäystapa on häiritä WLAN signaaleja suurella radiolähettimellä, joka estää signaalien kulkeutumista perille. (Geier 2016; F-Secure 2014.)

Vuoden 2016 lokakuussa suoritettiin maailman suurin palvelunestohyökkäys, jossa uhrina oli Dyn. Dyn on kansainvälinen internetin infrastruktuuria ylläpitävä yritys. Dynin asiakkaita ovat muun muassa Netflix, Spotify, Twitter ja Reddit.

Hyökkäys kohdistui IoT, eli Internet of Things -laitteisiin, jotka ohjattiin reitittämään liikenne Dynin DNS-nimipalvelujärjestelmään. Syy, miksi tämä hyökkäys oli mahdollinen, oli se, etteivät suurimmat osat koko maailman tukiasemista olleet tarpeeksi hyvin suojattuja.

Langattomien verkkojen tukiasemien perusasetuksia yksityiskäytössä ja julkisessa harvoin muutetaan. Hyökkäys pystyi murtautumaan ihmisten kotireitittimiin ja myös julkisiin reitittimiin käyttämällä oletusasetuksia: käyttäjänimellä admin ja salasanalla admin.

Kun murtautuminen oli suoritettu, laitteiden yhteydet ohjattiin Dynin nimpalvelujärjestelmään. Hyökkäykseen saatiin merkittävä määrä koko maailman IoT-laitteista, joka onkin syy, miksi Dyn: in palvelimet menivät alas. Yksityishenkilöllä ei voisi olla resursseja niin isoon palvelunestohyökkäykseen. (Wired 2016.)

3.4 Identiteettivarkaus (MAC-Spoofing)

Identiteettivarkaus onnistuu langattomissa verkoissa, joissa käytetään ainoastaan MAC-osoitteisiin perustuvaa pääsynhallintaa. Identiteettivarkaus tapahtuu siten, että hyökkääjä hankkii salakuuntelemalla haltuunsa langattoman verkon käyttöoikeuden omaavan laitteen MAC-osoitteen. Kyseisen osoitteen sekä tarvittavien ohjelmien avulla hyökkääjä voi halutessaan varastaa käyttöoikeuden omaavan laitteen käyttöoikeuden itselleen ja esiintyä verkossa laitteen käyttäjän identiteetillä. (Cardenas 2003.)

3.5 Verkkourkinta (Phishing)

Verkkourkinta on hyökkäysmenetelmä, jolla pyritään saamaan arkaluontoista tietoa uhrilta kuten esimerkiksi salasanoja ja luottokorttitietoja. Verkkourkintaa voi harrastaa monella eri tavalla, mutta tässä osiossa käsitellään menetelmä, joka liittyy suoraan julkisen verkon mahdollistamaan vaaraan. Se on usein myös liitoksissa Mies välissä -hyökkäykseen.

Hyökkäys alkaa sillä, että hyökkääjä katkaisee langattoman signaalin omalla signaalillaan, väärentää alkuperäisen verkon nimen ja korvaa sen sisäänkirjautumissivun omalla kopiollaan. Näin uhri, eli verkon käyttäjä, ajautuu väärennetylle langattomalle alueelle, missä uhri voidaan ohjata tietämättään erilaisille huijaussivustoille. Nämä huijaussivustot voivat sisältää erilaisia viruksia tai rekisteröitysmismahdollisuuksia, jolloin kaikki asiakkaan kenttiin syöttämät tiedot jäävät hyökkääjälle.

Ongelma tässä hyökkäyksessä uhrin kannalta on myös se, että jos hyökkääjä onnistuu vaihtamaan huijaussivustot uhrin selaimen välimuistiin, ei uhri ole turvassa edes julkisesta verkosta poistuttaessa. (Norton 2016.)

4 Julkisten WLAN-verkkojen tietoturvauhkien minimointi

Useissa WLAN-verkoissa tietoturva on jätetty lähestulkoon kokonaan käyttäjän vastuulle. Syynä on osittain se, että monimutkaisia ja tehokkaita verkon suojautumiskeinoja ei pystytä toteuttamaan julkisissa WLAN-verkoissa. Esimerkiksi WPA2 (Wi-Fi Protected Access 2), joka on yrityskäytössä yleisin langattoman verkon suojausmenetelmä, ei sovellu julkisiin hotspotteihin. Tämä johtuu siitä, että WPA2 on verkkovierailijoille liian hidas ja monimutkainen ottaa käyttöön.

Langaton verkkoyhteys voi olla avoin, jolloin liikennettä ei salakirjoiteta päätelaitteen ja tukiaseman välillä eikä yhteyden muodostamiseksi tarvita salasanaa. Salakirjoittamatonta dataa on äärimmäisen helppo salakuunnella. Julkisen langattoman verkon idea kuitenkin on se, että jokaisella taholla on mahdollisuus luoda yhteys, jolloin se on väkisinkin altis rikollisille. Langattoman verkon suojaamatta jättäminen myös helpottaa ja nopeuttaa verkkoon liittymistä huomattavasti.

Vaikka WLAN-verkko olisikin avoin, voi verkon tarjoaja kuitenkin vaatia käyttäjätunnuksen ja salasanan internetyhteyttä muodostaessa. Käyttäjä voidaan tässä tapauksessa ohjata kirjautumissivustolle, johon syötetään palvelun käyttäjätunnus ja salasana. Mutta kuten kappaleessa 3. todettiin, ei sekään tee yhteydestä täysin turvallista. Tässä kappaleessa käsitelläänkin siis sitä, kuinka julkisten langattomien lähiverkkojen tietoturvauhkia voidaan minimoida.

4.1 Käyttäjän asennoituminen tietoturvauhkiin

Tietoturvaa voi parantaa merkittävästi asentumalla oikein tietoturvaa kohtaan. Mikäli motivaatiota tietoturvan parantamista kohtaan ei ole, eikä myöskään tietoa mahdollisista tietoturvan riskeistä, käyttäjä asettaa itsensä alttiiksi uhkille. Suomalaisessa mediassa ei juurikaan julkisen verkon rikoksia ole tullut julki, vaan tapaukset pysyvät yleensä yksityisinä, mikä osaltaan on harmillista, sillä nykypäivänä ihmiset reagoivat vasta kun jotain sattuu. Esimerkiksi matkapuhelinten tietoturvaa laiminlyödään usein sillä perusteella, että laitteet eivät ole ennenkään suojattuja eikä mitään ole tapahtunut.

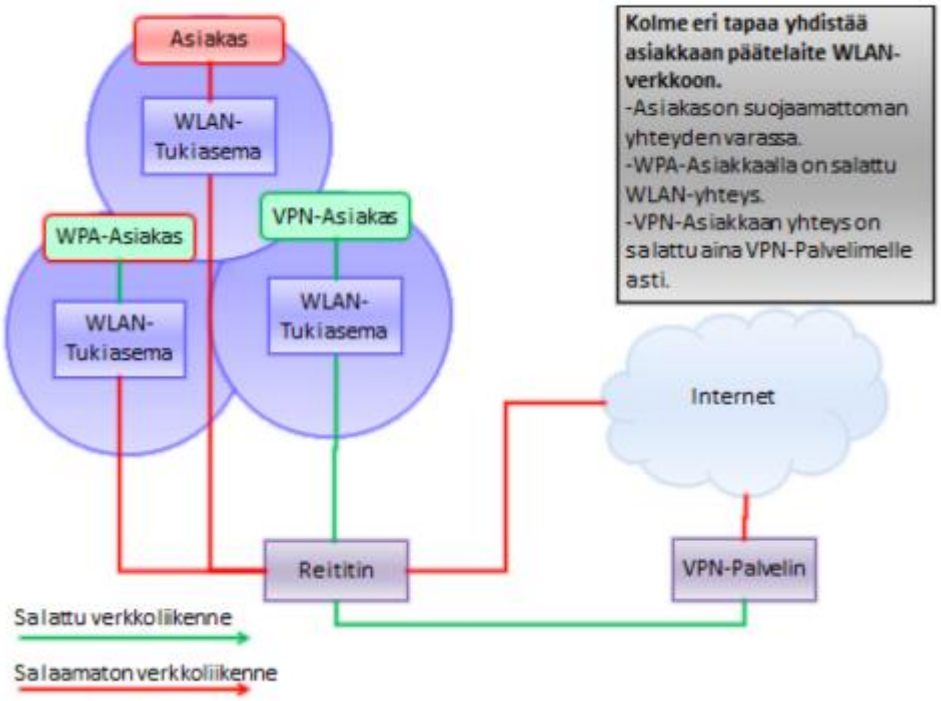
Myös normaali järjenkäyttö julkisissa WLAN-verkoissa on suositeltavaa. Pankkiasioita tai nettiostoksia ei kannata suorittaa julkisessa verkossa, sillä ne ovat suoraan alttiina rikollisilla.

4.2 Virtual Private Network (VPN)

VPN, eli virtuaalinen erillisverkko, tarjoaa käyttäjälle oikeastaan ainoan turvallisen tavan verkkovierailuun. Kun käyttäjä laittaa VPN-asetukset päälle, langattomassa verkossa kulkeva data on suojattu VPN-tunnelin avulla. VPN-tunneli toimii siten, että se kuljettaa salatun datan Internetin läpi haluttuun määränpäähän saakka (end-point). Tämä mahdollistaa sen, että hyökkääjät eivät kykene salakuuntelemaan käyttäjän yhteyttä.

Luotettavat VPN-asiakasohjelmat ovat usein maksullisia palveluita ja sen takia ne harvemmin ovatkaan yksityisasiakkaiden käytössä. Yrityksille VPN-yhteys on jo itsestään selvyys, koska se tarjoaa tärkeän suojan yhteydelle etätöitä tehdessä. On olemassa myös ilmaisia VPN-asiakasohjelmia, mutta sellaista hankittaessa tulee kuitenkin olla varuillaan. Sopivaa asiakasohjelmaa etsittäessä voi törmätä pahimmillaan pahantahtoisen tahon ylläpitämään vakoiluohjelmaan, jonka kautta voi ajautua suuriinkin ongelmiin.

Alla olevassa kuvassa selvennetään VPN-yhteyden tarjoamaa suojaa.



Kuvio 5. Eri tavat yhdistää WLAN-verkkoon. (Ekblad K, 2014.)

Kuvion 5. perusteella voidaan todeta VPN-tunneloinnin olevan erittäin tehokas tapa suojata yhteys. VPN-yhteys suojaa yhteyden aina VPN-palvelimelle asti.

4.3 Kaksivaiheinen tunnistautuminen

Tehokas tapa suojata verkossa olevat käyttäjätilit esimerkiksi mies välissä -hyökkäykseltä, kun niihin kirjaudutaan julkisessa verkossa, on kaksivaiheinen tunnistautuminen. Yleisin käytössä oleva menetelmä kaksivaiheisessa tunnistautumisessa on TOTP (Time-based One-Time Password). Se tarkoittaa sitä, että kun käyttäjä syöttää salasanansa palveluun, palveluntarjoaja lähettää automaattisesti 6-merkkisen pääsykoodin käyttäjän puhelimeen, jolla varmennetaan käyttäjän identiteetti. Pääsykoodi tulee siis matkapuhelinverkon kautta, eikä kyseisen langattoman lähiverkon kautta, joka tarkoittaa sitä, että vaikka käyttäjä olisikin uhrina

Mies välissä -hyökkäykselle, hyökkääjä ei pääse käsiksi uhrin käyttäjätiliin. TOTP mukaan pääsykoodi on yleensä määritelty vaihtuvan 30 sekunnin välein, jolloin hyökkääjällä on teoriassa 30 sekuntia aikaa kirjautua uhrin tilille.

Kaksivaiheinen tunnistautuminen on kuitenkin toistaiseksi palveluntarjoajasta riippuvainen, eikä käyttäjä voi vaikuttaa siihen, missä palveluissa hän haluaa sitä käyttää. Suosituksena kuitenkin on, että sitä käytetään kaikissa palveluissa, joissa se on mahdollista.

4.4 Salattu yhteys

Liikuttaessa Internetissä selaimella julkisessa WLAN-verkossa käyttäjän tulisi aina käyttää sivuja, joissa on HTTPS osoiterivin edessä. HTTPS on suojatun yhteyden protokolla Internetissä ja se salaa kaiken kommunikaation käyttäjän ja palvelimen välillä suojatakseen käyttäjää salakuuntelijoilta. HTTPS ohjaa selaimet käyttämään TLS-salausprotokollaa suojaamaan liikennettä. HTTP puolestaan on salaamaton, joten tämän suhteen käyttäjän tulee olla tarkkaavainen.

Verkko voidaan myös salata ylläpitäjän toimesta WEP-salauksella tai WPA- tai WPA2-salauksella. WEP-salaus on hieman vanhentunut, mutta se estää ensikertalaisten yritykset murtautua verkkoon, mutta ammattitaitoinen hakkeri murtautuu sen läpi helposti. WPA- ja WPA2-salaukset puolestaan suojaavat verkkoa hyvin, mutta hidastavat sen käyttöä. Toinen ongelma on myös siinä, että näitä salauksia käytettäessä tarvitaan yksi salasana langatonta verkkoa kohden. Esimerkiksi kahvilassa, työntekijät joutuisivat kertomaan jokaiselle asiakkaalle erikseen 26-merkkisen heksadesimaalisen WEP-avaimen ja mahdollisesti ratkomaan yhteysongelmia. Tässä tilanteessa yksinkertainen ratkaisu ilman salasanoja on helpompi ja vaivattomampi niin verkon ylläpitäjän kuin käyttäjänkin puolesta. Vaihtoehto kuitenkin on tarvittaessa saatavilla, ja se saattaakin sopia pienyrityksille kuten pienet kahvilat, lastentarhat ja lounaspaikat, joissa asiakaskunta on tuttu ja pienehkö.

Käyttäjän osalta kuitenkin paras vaihtoehto on turvautua VPN-yhteyden käyttöön yhteyden salaamiseksi, kuten aikaisemmin tässä opinnäytetyössä todettiin.

4.5 Tukiaseman asetukset

Tukiaseman asetukset eivät ole julkisen WLAN-verkon käyttäjän muokattavissa ja tästä syystä käyttäjä ei voi tähän asiaan vaikuttaa. Kuitenkin tukiaseman hallintasivustojen käyttäjätunnus- ja salasana -asetusten muuttaminen on niin tärkeä vaihe tietoturvallisuuden kannalta, että on perusteltua mainita se julkisten WLAN-verkkojen uhkien minimoimisessa. Mikäli näitä tunnuksia ei vaihdeta, on olemassa riski, että verkkoon tunkeutunut hyökkääjä voi halutessaan muuttaa tukiaseman kaikkia asetuksia. Mikäli tunkeutuja pääsee käsiksi pääsynhallintaan, voi hän muuttaa mielivaltaisesti tukiaseman asetuksia ja tehdä verkosta täysin turvattoman asiakkaille.

Usein tukiasemien oletus salasanat ja tunnukset löytyvät suoraan Internetistä. Tästä syystä on ehdottoman tärkeää, että ne muutetaan jo heti tukiaseman käyttöönoton yhteydessä. Kuten palvelunestokappaleessa mainittiin, yksityishenkilön tekemät suojatoimet voivat vaikuttaa pitkälti kaikkiin.

4.6 Lokitiedostot

Lokitiedostoja voidaan käyttää useissa langattoman verkon tukiasemissa. Lokitiedostot ovat tukiaseman kirjaamia langattomassa verkossa tapahtuneita aktiviteettejä ja niillä voidaan seurata esimerkiksi millä MAC-osoitteilla verkossa on asioitu. Tämän lisäksi lokitiedostoista on nähtävillä kaikki Internetistä tukiasemalle suuntautuneet hyökkäysyritykset sekä verkkoon tunkeutumiset.

Lokitiedostojen ansiosta voidaan myös tarkkailla reaaliajassa verkon aktiivisia laitteita ja verkkoliikennettä. Erillisillä seurantatyökaluilla voidaan selvittää kyseisellä hetkellä langattomassa verkossa vierailevien laitteiden verkko- sekä laiteosoitteet.

Lokitiedostoihin ei kuitenkaan ole tavallisella julkisen langattoman verkon käyttäjällä oikeuksia, mutta on hyvä tietää, että jos käyttäjä joutuu uhriksi, on hyökkäyksestä tai rikoksesta mahdollisesti näytettävää dataa todisteena verkon ylläpitäjällä.

5 Johtopäätökset

Julkisia hotspotteja löytyy kaikkialta. Ne mahdollistavat helpon pääsyn Internetiin ympäri maailmaa kaikille, jotka omaavat WLAN-teknologiaa tukevan päätelaitteen. Kuten työssä kuitenkin on todettu, WLAN-yhteyttä ei luotu turvallisuutta ajatellen, vaan se luotiin toiminnallisuutta ajatellen. Tästä syystä langattomalla lähiverkolla on omat hyvät sekä huonot puolensa. Hyviin puoliin voidaan lukea WLAN-verkon edullisuus sekä helppokäyttöisyys ja huonoihin puoliin sen sisältämät tietoturva-aukot.

Langalliseen verkkoon, eli LAN-verkkoon verrattuna suurimpana erona voidaan langattomissa verkoissa pitää tapaa, jolla tieto siirtyy. WLAN-tekniikassa käytettävät radioaallot ja niiden välityksellä kulkeva data ovat erittäin hankala suojata, koska niiden salakuunteleminen on vaivatonta ja huomaamatonta. Kiinteän verkon yhteyksiä on helpompi hallita ja käyttäjät voidaan identifioida.

Julkisessa verkossa verkon tarjoaja harvoin tarjoaa suojausta käyttäjälle. Yhteyden suojaaminen jätetään lähestulkoon aina käyttäjän vastuulle. Tästä johtuen suojaamattomissa julkisissa WLAN-verkoissa on aina vaara joutua hakkeroinnin tai salakuuntelun kohteeksi. Vaikka myös rikollisella on mahdollisuus jäädä kiinni, se mahdollisuus on hyvin pieni. Käyttäjän luotettava yksilöllinen identifiointi avoimessa julkisessa verkossa on hyvin hankalaa, jos ei jopa mahdotonta. Myöskään viranomaiset eivät yksittäistapauksissa puutu asiaan. Tämän lisäksi hyökkääjä voi myrkyttää käyttäjän laitteen julkisen verkon yli ja tehdä hyökkäyksen myöhemmin, mikä tekee hyökkääjän tunnistamisen vieläkin hankalammaksi. Nyt pitääkin siis alkaa kiinnittämään huomiota avoimiin julkisiin verkkoihin, sillä niiden kautta hakkerilla on mahdollisuus tehdä myös erittäin vakavia rikoksia.

En usko, että nykyisellä teknologialla pystyttäisi suojaamaan julkisia verkkoja ilman, että käyttäjä joutuu kyseisen suojauksen tekemään. Ainakin niin pitkään, kun verkon pitää olla helposti asiakkaiden saatavilla ongelma elää ja tietoturva on käyt-

täjän vastuulla. Uskon tulevaisuuden tuovan siihen ratkaisun, mutta sitä odotellessa jokainen, joka asioi julkisessa WLAN-verkossa on niin sanotusti vastuussa itsestään. Liitteenä on muistisäännöt siitä, kuinka yhdistää ja käyttää julkista verkkoa mahdollisimman turvallisesti.

Koen, että vaikka työ rajaa pois virustorjunnan, on siitä hyvä olla maininta. Virustorjuntaohjelmistot eivät varsinaisesti pysty suojaamaan käyttäjää hakkeroinnilta, mutta nämä ohjelmistot rajaavat haitalliset ja vihamieliset nettisivut ja ohjaavat käyttäjää asioimaan verkossa turvallisemmin. Sen lisäksi monessa virustorjuntaohjelmistossa on integroitu VPN, joka tekee yhteyden otosta mahdollisimman turvallisen.

Tämän työn tekeminen on auttanut minua ymmärtämään, kuinka suuri riski on yhdistää julkiseen verkkoon, mikäli tietotaitoa tietoturvasta ei ole. Tämä tieto on myös lisännyt mielenkiintoani aiheeseen ja täten edistänyt tutkimustani aiheesta laajemminkin. Kuitenkin rajausten ja selkeyden puitteissa osa tästä tiedosta on jätetty työstä pois. Omasta mielestäni työ kuitenkin on riittävän kattava henkilölle, joka on esimerkiksi samassa asemassa kuin minä itse ennen tutkimuksen aloittamista. Tällä kattavuudella tarkoitetaan siis sitä, että lukija ymmärtää riskit, miksi niitä on olemassa ja miten hän voi niiltä suojautua. Julkisissa WLAN-verkoissa surffaaminen riittämättömällä suojauksella saattaa aiheuttaa käyttäjälle suuriakin ongelmia, ja toivoakseni tämän työn avulla lukija ymmärtää ja osaa käsitellä aihetta asianmukaisesti.

Lähteet

Adding and securing a Public Wireless Access Point within a home network, Steven Christall, 2004. Luettavissa: https://www.sans.org/reading-room/whitepapers/casestudies/adding-securing-public-wireless-access-point-home-network-1551

Luettu: 29.6.2016

Asus 2016 Luettavissa:

https://www.google.fi/search?q=Asus+RT-AC66U&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiCq7Ca5MDPAhUBlS-wKHaaPC9EQ_AUICCgB&biw=1401&bih=780#imgrc=qmaGFyuQdeVzBM%3A

Luettu: 8.9.2016

Cisco 2016 Luettavissa:

https://www.google.fi/search?q=IBSS+,+BSS+and+ESS&espv=2&biw=1401&bih=780&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiOk-bWjrcTPAhWE_SwKHQ8xDyEQ_AUIBigB#imgrc=ENmNhPkDOb1c4M%3A

Luettu: 7.7.2016

Columbia University, Wireless Networking, Columbia yliopiston www-sivut. 2016 Luettavissa:

http://cuit.columbia.edu/network-wireless-services

Luettu: 29.6.2016

Denial of Service a Big WLAN Issue, Jim Geier, eSecurity Planet, 2003. Luettavissa: http://www.esecurityplanet.com/trends/article.php/2200071/Denial-of-Service-a-Big-WLAN-Issue.htm

Luettu: 10.10.2016

Exploiting and Protecting 802.11b Wireless Networks, Ellison Craig, 2001. Luettavissa: http://www.extremetech.com/computing/57646-exploiting-and-protecting-80211b-wireless-networks

Luettu: 22.7.2016

F-Secure 2014, Wi-fi Report 2014. Luettavissa: https://fsecureconsumer.files.wordpress.com/2014/09/wi-fi_report_2014_f-secure.pdf

Luettu: 29.6.2016

How an attacked could crack your wireless network security, Chris Hoffman, 2016. Luettavissa:

http://www.howtogeek.com/191482/how-an-attacker-could-crack-your-wireless-network-security/

Luettu: 10.10.2016

Internetopas 2016, Tietoturva, Internetopas www-sivut. Luettavissa: http://www.internetopas.com/yleistietoa/tietoturva/

Luettu: 1.7.2016

Jimms 2016 Luettavissa:

https://www.jimms.fi/fi/Product/Show/74298/rt-ac66u/asus-rt-ac66u-langaton-ac1750-dual-band-tukiasema-2_4-5ghz-802_11ac-testimenestyja

Luettu: 20.10.2016

John Hopkins School of Public Health 2016, Wireless Networking History. Luettavissa: www.jhsph.edu/wireless/history.html

Luettu: 1.8.2016

Man in the Middle Attack, Neil DuPaul, 2016. Luettavissa:

http://www.veracode.com/security/man-middle-attack

Luettu: 10.10.2016

MAC Spoofing -- An Introduction, Edgar D Cardenas, Sans Institute, 2003. Luettavissa:

https://www.giac.org/paper/gsec/3199/mac-spoofing-an-introduction/105315

Luettu: 10.10.2016

Norton 2016, Langattomat Wi-Fi-alueet: yhteydet matkoilla. Luettavissa:

https://fi.norton.com/travel-hotspot-security/article

Luettu: 28.7.2016

Protecting from the dangers of corporate users accessing WiFi hotspots, Ed Fisher, Sans Institute, 2005. Luettavissa: https://www.giac.org/paper/gsec/4267/protecting-dangers-corporate-users-accessing-wifi-hotspots/106913#__utma=216335632.885550917.1460614561.1470994713.1474215413.4&__utmb=216335632.12.9.1474215499247&__utmc=216335632&__utmx=-&__utmz=216335632.1460614561.1.1.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided)&__utmv=-&__utmk=207831633

Luettu: 29.6.2016

Raymond 2016 Luettavissa:

https://www.raymond.cc/blog/how-to-discover-hidden-wireless-network/

Luettu 20.10.2016

Sans Institute 2015b, Wi-Fi Security Newsletter. Luettavissa:

https://securingthehuman.sans.org/media/services/Module11-WiFiSecurity-Newsletter.pdf#__utma=216335632.2024781096.1461570870.1461570870.1461570870.1&__utmb=216335632.5.8.1461570893500&__utmc=216335632&__utmx=-&__utmz=216335632.1461570870.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none)&__utmv=-&__utmk=237117635

Luettu: 1.7.2016

SecurEnvoy 2016, What is Two-Factor Authentication? Luettavissa:
https://www.securenvoy.com/two-factor-authentication/what-is-2fa.shtm

Luettu: 15.10.2016

Symantec 2008, Varo langattoman verkon vaaroja. Luettavissa:
http://www.symantec.com/region/fi/resources/wireless.html

Luettu: 14.8.2016

Technopedia 2016, Wireless Local Area Network. Luettavissa: https://www.techopedia.com/definition/5107/wireless-local-area-network-wlan

Luettu: 1.8.2016

Veracode 2016 Luettavissa:

http://www.veracode.com/security/man-middle-attack

Luettu: 20.10.2016

Viestintävirasto 2014, Langattomasti mutta turvallisesti. Luettavissa: https://www.viestintavirasto.fi/attachments/tietoturva/Langattomasti_mutta_turvallisesti._Langattomien_lahiverkkojen_tietoturvallisuudesta.pdf

Luettu: 1.7.2016

Wardrive 2016, Wardrive www-sivut. Luettavissa:

http://www.wardrive.net/wardriving/faq

Luettu: 10.10.2016

Webopedia 2016a, What is Wi-Fi (IEEE 802.11x)? Luettavissa:

http://www.webopedia.com/TERM/W/Wi_Fi.html

Luettu: 28.7.2016

Webopedia 2016b, Wireless networks explained. Luettavissa:

http://www.webopedia.com/DidYouKnow/Computer_Science/wireless_networks_explained.asp

Luettu: 28.7.2016

Wikipedia Luettavissa:

https://en.wikipedia.org/wiki/IEEE_802.11

Luettu: 1.8.2016

WiMAX: Technology for Broadband Wireless Access, Nuaymi Loutfi, 2007. Luettu: 29.6.2016

Wired: What we know about Friday's massive east coast Internet outage, 2016. Luettavissa: https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/

Luettu: 22.10.2016

Wireless LAN Site 2009, WLAN Topologies. Luettavissa: http://wireless-lansite.blogspot.fi/2009/07/wlan-topologies.html

Luettu: 8.9.2016

Wireless LAN: Security Issues and Solutions, Rafidah Abdul Hamid, Sans Institute, 2003. Luettavissa:

https://www.sans.org/reading-room/whitepapers/wireless/wireless-lan-security-issues-solutions-1009

Luettu: 20.9.2016

Wireless Networks: Security Problems and Solutions, Jonathan Weiss, Sans Institute, 2002. Luettavissa: https://www.sans.org/reading-room/whitepapers/wireless/wireless-networks-security-problems-solutions-172

Luettu: 29.6.2016

Wi-Fi Alliance 2016, Who we are. Luettavissa:

http://www.wi-fi.org/who-we-are

Luettu: 1.8.2016

WLAN-verkon suojaus VPN-yhteyden avulla, Ekblad Kim, 2014. Luettavissa:

https://publications.theseus.fi/bitstream/handle/10024/77274/Ekblad_Kim.pdf?sequence=1

Luettu: 20.10.2016

Liitteet

Liite 1. Tietoturvaohjeet yhdistäessä julkiseen langattomaan lähiverkkoon

1. Varmista paikan henkilökunnalta tai suoraan langattoman verkon tarjoajalta heidän käyttämä virallinen nimi langattomalle verkolle. Näin varmistat, ettet vahingossa yhdistä kenenkään kolmannen osapuolen luomaan vihamieliseen langattomaan verkkoon.

2. Valitse paikkasi langattoman verkon kantoalueella tarkkaan siten, että kukaan ei pääse seuraamaan tekemisiäsi tai urkkimaan salasanojasi, kun asioit verkossa.

3. Varmista, että laitteesi virusturva on ajan tasalla. Tämä estää sinua esimerkiksi ajautumasta haittasivuille, vaikka yhteytesi ei olisikaan salattu.

4. Kytke VPN päälle. Näin suojaat yhteytesi ja estät muita sieppaamasta ilmassa liikkuvaa dataa.

5. Käytä maalaisjärkeä asioidessasi julkisessa WLAN-verkossa. Pankkiasiat ja esimerkiksi verkkokauppaostokset kannattaa hoitaa vasta turvallisessa verkossa. Riski tietojen menetykseen julkisessa verkossa on huomattavasti suurempi kuin esimerkiksi yksityishenkilön kotiverkossa.